IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s)	:	Conrado et al.
Serial No.	:	10/549,885
Filed	:	September 16, 2005
For	:	User Identity Privacy in Authorization Certificates
Group Art Unit	:	2431
Examiner	:	Brett S. Squires
Confirmation	:	7551

Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUBMISSION OF REQUEST FOR CONTINUED EXAMINATION (RCE) AND RESPONSE TO MAY 29, 2009 ADVISORY ACTION

A Final Office Action was issued on March 9, 2009, and an Amendment and/or Response to such Final Office Action was filed on May 11, 2009.

The Advisory Action that issued on May 29, 2009 indicated that the Amendment and/or Response filed on May 11, 2009 "will be entered" for purposes of appeal. The Advisory Action lists currently-pending claims 1-10 and 12-32 as being rejected. No further amendments to the claims are made herewith.

In response to the Advisory Action issued on May 29, 2009, and in conjunction with the concurrent filing of a Request for Continued Examination, please consider the remarks presented herein. A Request for Continued Examination (RCE) is enclosed and submitted herewith, together with payment of the official fee of $810.00 specified in 37 CFR 1.17(e) applicable to a large entity.

I. INTRODUCTION

Claims 1-10 and 12-32 are currently pending in the application. Claims 1, 22, 25, and 26 having been amended in connection with Applicants' submission dated May 11, 2009; such amendments were entered as indicated in the Advisory Action.

The May 29, 2009 Advisory Action stated at page 3 thereof that:

> "[T]he examiner respectfully points out that the applicants' argument relies heavily on information from Wikipedia. The examiner now points out that Wikipedia has been removed from the U.S. Patent and Trademark Office's list of accepted sources of information and therefore arguments based on information from Wikipedia are not persuasive."

Applicants rely herein on sources of information beyond Wikipedia, thereby eliminating the sole basis raised in the Advisory Action for preventing allowance of Applicants' claims.

All of the outstanding claim rejections are traversed for the reasons set out below.

II. THE CLAIM REJECTIONS UNDER 35 U.S.C. § 103(a) SHOULD BE WITHDRAWN

The March 9, 2009 Final Office Action contained multiple rejections under 35 U.S.C. § 103(a), namely:

- a rejection of claims 1-2, 5-9, 12-19, 22-26, and 29-32[1] as being unpatentable for obviousness over Saito et al. "Privacy Enhanced Access Control by SPKI" (hereinafter "Saito") in view of U.S. Patent No, 5,717,758 to Micall (hereinafter "Micall");
- a rejection of claims 3-4, 10, 20-21, and 27-28[2] as being unpatentable for obviousness over Saito in view of Micall, and further in view of U.S. Patent Application Publication No. 2007/0189542 to Alldredge (hereinafter "Alldredge").

[1] See 03/09/09 Office Action, pp. 2-9.
[2] See 09/09/09 Office Action, pp. 9-11.

Such rejections are traversed.

In the March 9, 2009 Final Office Action, the examiner conceded that "Saito does not disclose reissuing associations between user identifying information and data" (March 9, 2009 Office Action, page 2), but alleged that it would be obvious to combine Micall with Saito to yield the subject matter of Applicants' independent claims. As detailed below, Saito relates to Simple Public Key Infrastructure (SPKI), while Micall relates to Public Key Infrastructure ("PKI"), such that Micall is not properly combinable with Saito to support the rejection of any of Applicants' independent claims. The distinctions between PKI and SPKI are discussed below to provide appropriate background for the impropriety of combining the disclosures of Micall and Saito.

A. Discussion of Public Key Infrastructure (PKI) and Simple Public Key Infrastructure (SPKI)

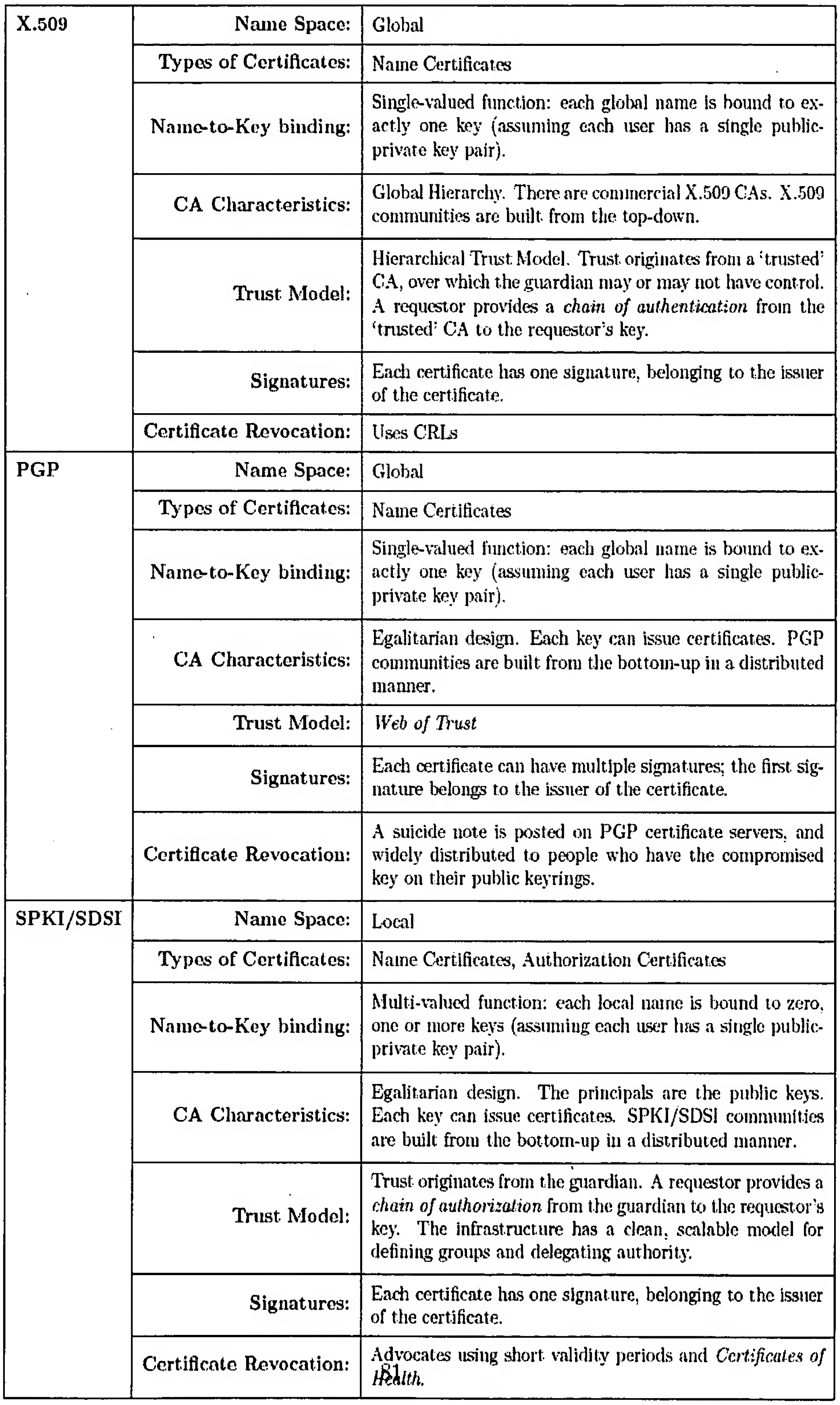
It is generally understood in the art that both Public Key Infrastructure ("PKI") and Simple Public Key Infrastructure ("SPKI") represent different authentication solutions, with PKI utilizing a certificate authority (CA) that binds public keys with user identities, but with SPKI eliminating the need for any certificate authority by use of an authorization loop (whereby the verifier is also the issuer (such that public authentication of public key information, and use of a certificate authority, is *unnecessary*). See, e.g., the following excerpts:

> SPKI/SDSI (Simple Public Key Infrastructure/Simple Distributed Security Infrastructure): The SPKI efforts of the IETF have been combined with SDSI, an approach outlined by MIT's Ron Rivest and Microsoft's Butler Lampson. ... **SDSI/SPKI differs from the more developed and accepted PKIX (Public Key Infrastructure X.509) in specifying a highly distributed, client-focused trust model** relying on delegated human-readable certificates. For example, a business might issue "salesperson" certificates to employees and those employees might issue "salesperson-customer" certificates to customers, and only those customers identified as customers associated with a salesperson will gain entry. SDSI/SPKI also is more flexible than PKIX in letting end users define rules for processing certificates. It also rejects the complex ASN.1

> syntax of X.509. **Considerable control is put in the hands of end users, rather than relying on a centralized infrastructure for establishing identities**. The infrastructure also puts an emphasis on short-lived, ephemeral certificates, reissued daily, for example, in lieu of extensive reliance on CRLs.

Source: Network Computing "Certificate Authority Glossary," available online at http://www.networkcomputing.com/813/813f2glos.html (emphasis added).

See also Clarke, "SPKI/SDSI HTTP Server / Certificate Chain Discovery in SPKI/SDSI," Thesis Submitted to Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Sept. 2001, page 81, table 3.1, (available online at http://groups.csail.mit.edu/cis/theses/clarke-masters.pdf) as reproduced below.



X.509	**Name Space:**	Global
	Types of Certificates:	Name Certificates
	Name-to-Key binding:	Single-valued function: each global name is bound to exactly one key (assuming each user has a single public-private key pair).
	CA Characteristics:	Global Hierarchy. There are commercial X.509 CAs. X.509 communities are built from the top-down.
	Trust Model:	Hierarchical Trust Model. Trust originates from a 'trusted' CA, over which the guardian may or may not have control. A requestor provides a *chain of authentication* from the 'trusted' CA to the requestor's key.
	Signatures:	Each certificate has one signature, belonging to the issuer of the certificate.
	Certificate Revocation:	Uses CRLs
PGP	**Name Space:**	Global
	Types of Certificates:	Name Certificates
	Name-to-Key binding:	Single-valued function: each global name is bound to exactly one key (assuming each user has a single public-private key pair).
	CA Characteristics:	Egalitarian design. Each key can issue certificates. PGP communities are built from the bottom-up in a distributed manner.
	Trust Model:	*Web of Trust*
	Signatures:	Each certificate can have multiple signatures; the first signature belongs to the issuer of the certificate.
	Certificate Revocation:	A suicide note is posted on PGP certificate servers, and widely distributed to people who have the compromised key on their public keyrings.
SPKI/SDSI	**Name Space:**	Local
	Types of Certificates:	Name Certificates, Authorization Certificates
	Name-to-Key binding:	Multi-valued function: each local name is bound to zero, one or more keys (assuming each user has a single public-private key pair).
	CA Characteristics:	Egalitarian design. The principals are the public keys. Each key can issue certificates. SPKI/SDSI communities are built from the bottom-up in a distributed manner.
	Trust Model:	Trust originates from the guardian. A requestor provides a *chain of authorization* from the guardian to the requestor's key. The infrastructure has a clean, scalable model for defining groups and delegating authority.
	Signatures:	Each certificate has one signature, belonging to the issuer of the certificate.
	Certificate Revocation:	Advocates using short validity periods and *Certificates of Health.*

Table 3.1: Comparison of X.509, PGP, and SPKI/SDSI

The foregoing table summarizes stark differences between PKI ("X.509") and SPKI with respect to Certificate Authority (CA) Characteristics and Trust Model. As indicated above, PKI (X.509) employs a Certificate Authority having a "global hierarchy" with commercial certificate authorities and communities that are built from the top down. In contrast, a SPKI structure is characterized by an "egalitarian design" wherein the principals are the public keys and each key can issue certificates, with SPKI communities being built from the bottom-up in a distributed manner. The trust model used by PKI (X.509) is a hierarchical trust model with trust originating from the Certificate Authority (CA), and with a requestor providing a chain of authenticity from the 'trusted' CA to the requestor's key. In contrast, SPKI utilizes a trust model in which trust originates from the guardian. A requestor provides a chain of authorization from the guardian to the requestor's key. As a result, SPKI has no need for a commercial CA.

It is noted that Wikipedia also provides a discussion of Public Key Infrastructure and Simple Public Key Infrastructure that is consistent with the foregoing references[3,4,5].

B. No Basis Exists for the Hypothetical Combination of Saito and Micall

[3] "A Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates. A PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique for each CA. The binding is established through the registration and issuance process, which, depending on the level of assurance the binding has, may be carried out by software at a CA, or under human supervision. The PKI role that assures this binding is called the Registration Authority (RA). For each user, the user identity, the public key, their binding, validity conditions and other attributes are made unforgeable in public key certificates issued by the CA. The term trusted third party (TTP) may also be used for certificate authority (CA)." (*See* http://en.wikipedia.org/wiki/Public_key_infrastructure.)

[4] "An alternative approach to the problem of public authentication of public key information ... which however does not deal with public authentication of public key information, is the simple public key infrastructure ("SPKI") that grew out of 3 independent efforts to overcome the complexities of X.509 and PGP's web of trust. SPKI does not bind people to keys, as the key is what is trusted, rather than the person. SPKI does not use any notion of trust, as the verifier is also the issuer. This is called an "authorization loop" in SPKI terminology, where authorization is integral to its design." (*See* http://en.wikipedia.org/wiki/Public_key_infrastructure.)

[5] SPKI specification defines an authorization certificate format, providing for the delineation of privileges, rights or other such attributes (called authorizations) and binding them to a public key. [SPKI] does not define a role for a commercial Certificate Authority (CA). In fact, **one premise behind SPKI is that a commercial CA serves no useful purpose**. (*See* http://en.wikipedia.org/wiki/Simple_public_key_infrastructure.)

Saito is directed to a privacy enhanced service scheme utilizing Simple Public Key Infrastructure (SPKI). Saito describes his privacy-enhanced access control system provides the useful property of being "light and efficien[t]," specifically stating the following:

> "Since public key is **not mapped to ID** in an SPKI certificate, public key can be generated for a service or a set of services and discarded after its usage or lifetime. This **disposable** key scheme alleviates the management of public keys."

(Saito, pg. 302, second column.)

Saito describes another useful property of his privacy-enhanced access control system as being "self-verifiable," specifically stating the following:

> "In the SPKI scheme, there is a chain of verification: **without a server's or third party's help, clients can verify certificates by themselves.**"

(Saito, pg. 302, second column.)

In contrast to the SPKI-based system of Saito, Micall is directed to a traditional PKI-based system involving a certificate authority (CA), wherein an intermediary (a "witness") processes authenticated certificate information to construct authenticated deduced information. Such a witness system enables users to save transmission costs of certificate information (e.g., reducing need to transmit a long Certificate Revocation List (CRL), or search the CRL, to establish whether a given certificate has been revoked). An advantage of a witness system according to Micall is that, in comparison to direct communication with a CA, the intermediary provides much shorter answers when authenticating the status of issued certificates. (Micall, col. 8, lines 38-45.)

To support the hypothetical combination of Micall and Saito, the examiner stated:

> "It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the privacy enhanced access control by simple public key infrastructure [of Saito] to include reissuing valid SPKI certificates such as that taught by Micall in order [to] reduce processing overhead by reissuing valid certificate instead of generating a new certificate."

(March 9, 2009 Office Action, page 3).

The foregoing rationale advanced by the examiner for combining Micall and Saito fails in multiple respects.

First, Saito specifically relates to a *SPKI-based* system (i.e., lacking a Certificate Authority), whereas Micall specifically relates to a *PKI-based* system that requires a Certificate Authority. Various fundamental differences between SPKI-based and PKI-based systems are identified hereinabove, but apparently have been overlooked by the examiner. For example, Micall requires a Certificate Authority, whereas Saito specifically does not require help from a server or third party (e.g., a Certificate Authority) to verify certificates. (See Saito, pg. 302, second column.) Given the fundamental differences between the two references, there is no indication that the PKI-based system of Micall would be compatible with the SPKI-based system of Saito to produce an operative combined system. A proposed combination of references that would produce a "seemingly inoperative" system cannot support a *prima facie* case of obviousness under 35 U.S.C. 103[6]. Accordingly, the proposed combination of Micall and Saito is not supportable.

Second, Saito specifically his SPKI system as being advantageous because it utilizes a disposable key scheme that alleviates the management of public keys (See Saito, pg. 302, second column.) This directly contradicts the examiner's assertion that one skilled in the art would combine Micall with Saito to reduce processing overhead, since addition of Micall's PKI-based complex key management system (i.e., requiring a Certificate Authority) would increase processing overhead. The obviousness rejections premised on the hypothetical combination of Saito and Micall are erroneous for at least the reason that the examiner has failed to consider portions of Saito that teach away from

[6] The Federal Circuit and its predecessor court have repeatedly held that **if references taken in combination would produce a 'seemingly inoperative' device, then such references teach away from the combination** and cannot serve as predicates for a *prima facie* case of obviousness. *McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339, 60 USPQ2d 1001, 1010 (Fed. Cir. 2001); *Tec Air, Inc. v. Denso Mfg. Mich. Inc.*, 192 F.3d 1353, 52 USPQ2d 1294, 1298 (Fed. Cir. 1999) (proposed combination of references that would be inoperable for intended purpose supports teaching away from combination); *In re Gordon*, 733 F.2d 900, 902, 221 USPQ 1125, 1127 (Fed. Cir. 1984) (inoperable modification teaches away); *In re Sponnoble*, 405 F.2d 578, 587, 160 USPQ 237, 244 (C.C.P.A. 1969) (references teach away from combination if combination produces seemingly inoperative device).

the combination[7]. Given such teaching away, the examiner's rationale supporting the hypothetical combination of references does not embody "articulated reasoning with some rational underpinning to support the legal conclusion of obviousness," as required by the Supreme Court in *KSR International Co. v. Teleflex Inc.*, 127 S.Ct 1727, 167 L.Ed.2d 705, 82 USPQ2d 1385, 1396 (2007).

Each of claims 1, 22, 29, 30, 31, and 32 is allowable over Saito for at least the reason that Saito fails to disclose the feature of "wherein the concealing data remains fixed for reissued associations." As the rejections of Applicants' independent claims 1, 22, 29, 30, 31, and 32 under 35 U.S.C. 103 are all premised on the hypothetical combination of Micall and Saito, and it has been demonstrated that such hypothetical combination of Micall and Saito is insupportable, no basis remains for maintaining such claim rejections.

In the March 9, 2009 Final Office Action, the examiner has cited Alldredge as allegedly disclosing (1) "a cryptographic system that encrypts a users message using a symmetric key," (2) "a method·for secured electronic commerce using sequences of one time pads for concealing transmitted messages," and (3) a cryptographic system that includes a secret security identifier[8]," as relating to claims 3-4, 10, 20-21, and 27-28. Alldredge fails to support any hypothetical combination of Micall or Saito, or to remedy the deficiencies of Saito (or Micall) in disclosing all elements of Appliant's independent claims 1, 22, 29, 30, 31, and 32.

Accordingly, withdrawal of the rejections of Applicants' independent claims 1, 22, 29, 30, 31, and 32 is warranted, and is respectfully requested. Since dependent claims inherently include all of the features of the claims on which they depend[9], all claims depending (whether directly or indirectly) from independent claims 1, 22, 29, 30, 31, and

[7] In considering a reference for its effect on patentability, the reference is required to be considered in its entirety, including portions that **teach away** from the invention under consideration. Simply stated, the prior art must be considered as a whole. *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984) (emphasis added); MPEP § 2141.02. "It is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art." *Application of Wesslau*, 353 F.2d 238, 241 (C.C.P.A. 1965); *Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve*, 796 F.2d 443, 448 (Fed. Cir. 1986), cert. denied, 484 U.S. 823 (1987).

[8] March 9, 2009 Final Office Action, pages 10-11.

[9] 35 U.S.C. 112, fourth paragraph.

32 are likewise patentably distinguished over the cited art. Withdrawal of the rejectiosn of all dependent claims is warranted, and is respectfully requested.

CONCLUSION

In light of the foregoing, Applicants respectfully submit that all of the now-pending presented claims are in condition for allowance. Examination of the enclosed claims and issuance of a notice of allowance are earnestly solicited. Should any issues remain that may be amenable to telephonic resolution, the examiner is invited to telephone the undersigned attorneys to resolve such issues as expeditiously as possible.

In the event there are any errors with respect to the fees for this response or any other papers related to this response, the Director is hereby given permission to charge any shortages and credit any overcharges of any fees required for this submission to Deposit Account No. 14-1270.

Respectfully submitted,

By: /vincent k. gustafson/
Vincent K. Gustafson
Registration No.: 46,182

Dated: June 9, 2009

INTELLECTUAL PROPERTY/
TECHNOLOGY LAW
P.O. Box 14329
Research Triangle Park, NC 27709
Phone: 919-419-9350

For: Kevin C. Ecker
Registration No.: 43,600
Phone: (914) 333-9618

Please direct all correspondence to:
Kevin C. Ecker, Esq.
Philips Intellectual Property & Standards
P.O. Box 3001
Briarcliff Manor, NY 10510-8001